certification is withdrawn, DEA will also provide written notice to the bidder and end-user, which will contain a statement of the legal and factual basis for this determination.

(e) If the Administrator determines there is reasonable cause to believe the sale of the specific chemical to a specific bidder and end-user would result in the illegal manufacture of a controlled substance, DEA will provide written notice to the head of a Federal department or agency refusing to certify the proposed sale under the authority of 21 U.S.C. 890. DEA also will provide, within fifteen calendar days of receiving a request for certification from a Federal department or agency, the same written notice to the prospective bidder and end-user, and this notice also will contain a statement of the legal and factual basis for the refusal of certification. The prospective bidder and end-user may, within thirty calendar days of receipt of notification of the refusal, submit written comments or written objections to the Administrator's refusal. At the same time, the prospective bidder and end-user also may provide supporting documentation to contest the Administrator's refusal. If such written comments or written objections raise issues regarding any finding of fact or conclusion of law upon which the refusal is based, the Administrator will reconsider the refusal of the proposed sale in light of the written comments or written objections filed. Thereafter, within a reasonable time, the Administrator will withdraw or affirm the original refusal of certification as he determines appropriate. The Administrator will provide written reasons for any affirmation of the original refusal. Such affirmation of the original refusal will constitute a final decision for purposes of judicial review under 21 U.S.C. 877.

(f) If the Administrator determines there is reasonable cause to believe that an existing certification should be withdrawn, DEA will provide written notice to the head of a Federal department or agency of such withdrawal under the authority of 21 U.S.C. 890. DEA also will provide, within fifteen calendar days of withdrawal of an existing certification, the same written notice to the bidder and end-user, and this notice also will contain a statement of the legal and factual basis for the withdrawal. The bidder and end-user may, within thirty calendar days of receipt of notification of the withdrawal of the existing certification, submit written comments or written objections to the Administrator's withdrawal. At the same time, the bidder and end-user also may provide supporting documentation to contest the Administrator's withdrawal. If such written comments or written objections raise issues regarding any finding of fact or conclusion of law upon which the withdrawal of the existing certification is based, the Administrator will reconsider the withdrawal of the existing certification in light of the written comments or written objections filed. Thereafter, within a reasonable time, the Administrator will withdraw or affirm the original withdrawal of the existing certification as he determines appropriate. The Administrator will provide written reasons for any affirmation of the original withdrawal of the existing certification. Such affirmation of the original withdrawal of the existing certification will constitute a final decision for purposes of judicial review under 21 U.S.C. 877.

[68 FR 62737, Nov. 6, 2003]

PART 1311—DIGITAL CERTIFICATES

Subpart A—General

Sec.

Subpart B—Obtaining and Using Digital Certificates for Electronic Orders

AUTHORITY: 21 U.S.C. 821, 828, 829, 871(b), 958(e), 965, unless otherwise noted.

SOURCE: 70 FR 16915, Apr. 1, 2005, unless otherwise noted.

EFFECTIVE DATE NOTE: At 70 FR 16915, Apr. 1, 2005, part 1311 was added, effective May 31, 2005.

Subpart A—General

§ 1311.01 Scope.

This part sets forth the rules governing the use of digital signatures and the protection of private keys by registrants.

§ 1311.02 Definitions.

For the purposes of this chapter:

Biometric authentication means authentication based on measurement of the individual's physical features or repeatable actions where those features or actions are both unique to the individual and measurable.

Cache means to download and store information on a local server or hard drive.

Certificate Policy means a named set of rules that sets forth the applicability of the specific digital certificate to a particular community or class of application with common security requirements.

Certificate Revocation List (CRL) means a list of revoked, but unexpired certificates issued by a Certification Authority.

Certification Authority (CA) means an organization that is responsible for verifying the identity of applicants, authorizing and issuing a digital certificate, maintaining a directory of public keys, and maintaining a Certificate Revocation List.

CSOS means controlled substance ordering system.

Digital certificate means a data record that, at a minimum:

(1) Identifies the certification authority issuing it;

(2) Names or otherwise identifies the certificate holder;

(3) Contains a public key that corresponds to a private key under the sole control of the certificate holder;

(4) Identifies the operational period; and

(5) Contains a serial number and is digitally signed by the Certification Authority issuing it.

Digital signature means a record created when a file is algorithmically transformed into a fixed length digest that is then encrypted using an asymmetric cryptographic private key associated with a digital certificate. The combination of the encryption and algorithm transformation ensure that the signer's identity and the integrity of the file can be confirmed.

Electronic signature means a method of signing an electronic message that identifies a particular person as the source of the message and indicates the person's approval of the information contained in the message.

FIPS means Federal Information Processing Standards. These Federal standards, as incorporated by reference in §1311.08, prescribe specific performance requirements, practices, formats, communications protocols, etc., for hardware, software, data, etc.

FIPS 140–2, as incorporated by reference in §1311.08, means a Federal standard for security requirements for cryptographic modules.

FIPS 180–2, as incorporated by reference in §1311.08, means a Federal secure hash standard.

FIPS 186–2, as incorporated by reference in §1311.08, means a Federal standard for applications used to generate and rely upon digital signatures.

Key pair means two mathematically related keys having the properties that:

(1) One key can be used to encrypt a message that can only be decrypted using the other key; and

(2) Even knowing one key, it is computationally infeasible to discover the other key.

NIST means the National Institute of Standards and Technology.

Private key means the key of a key pair that is used to create a digital signature.